View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Purdue E-Pubs

Purdue University

Purdue e-Pubs

Department of Computer Science Technical Reports

Department of Computer Science

1989

Computer Vandalism and the Law

Eugene H. Spafford
Purdue University, spaf@cs.purdue.edu

Report Number:
89-936

Spafford, Eugene H., "Computer Vandalism and the Law" (1989). *Department of Computer Science Technical Reports.* Paper 796.
https://docs.lib.purdue.edu/cstech/796

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.

COMPUTER VANDALISM AND THE LAW

Eugene H. Spafford

CSD-TR-936
November 1989

Computer Vandalism and the Law[1]

Purdue University Technical Report CSD-TR-936

Eugene H. Spafford

28 November 1989

[1]© Copyright 1989 by ADAPSO, Inc. and Eugene H. Spafford. All rights reserved.

Abstract

There has been considerable interest of late in computer viruses, computer break-ins, and other forms of electronic vandalism. One of the concerns often expressed by victims (and potential victims) is how the laws deal with these malicious acts.

This report is a brief introduction to some of the possibilities, alternatives, and problems of applying the legal system to incidents of computer vandalism. It briefy surveys some of the important aspects of criminal and civil prosecution, and provides a comprehensive list of state and federal statutes that might be brought to bear in cases of computer crime.

The interested reader is directed to the book from which this report is derived for further information, including references to related works and sources, and technical information on computer viruses: *Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats*, E. H. Spafford, K. A. Heaphy, and D. J. Ferbrache, ADAPSO, 1989.

1 Introduction

Technological methods are not the only means of lessening your risk and preventing losses from computer viruses and "crackers," just as using stronger bank vaults or better door locks are not the only means of discouraging individuals from robbing banks or breaking into our homes. We use the legal system to increase the risk and cost associated with activities that we consider contrary to proper behavior.

In this report, we will outline the difficulties involved in using legal methods against virus authors and users. We will look exclusively at the U.S. legal system because of the complexity and variability of laws in other countries. The purpose of this report is not so much to outline legal strategy, but to make you aware of the possibilities and difficulties associated with these approaches. If you wish to investigate this topic further, Appendix A lists particular resources you can use. It would be inappropriate to go into any amount of detail here because the laws and legal precedents involved are complex, and vary considerably from locality to locality. If you need more detailed information, you should contact an attorney in your area who is particularly well-versed in business and criminal law. Certainly, you should contact members of appropriate law enforcement agencies as well.

2 Approaches

There are two legal approaches that can be used separately or in combination with each other to discourage virus writers and computer vandals: civil action and criminal action. First we will discuss criminal law, and laws that can be used against authors of computer viruses and other forms of computer security threats.

2.1 Criminal laws

2.1.1 Federal law

Criminal laws are passed by elected representatives to codify the most egregious of inappropriate, unacceptable behavior, and to specify remedies and penalties to discourage that behavior. There are federal and state laws that deal with computer tampering, and even some municipal laws that apply. The federal laws govern offenses that deal with federal property, national security, national interests, or that affect interstate commerce or communi-

cations. To apply these laws requires evidence that the individuals involved have trespassed into or tampered with computers that are federal property, owned or run by a federal agency, or considered to be federal interest computers (such as computers in credit unions or banks). If the computer access affects interstate commerce or national security, then various federal regulations also apply, and those activities may be investigated and prosecuted in federal court. Many laws not specifically directed at computer crime may also be used to prosecute these offenses.

The Federal Computer Fraud and Abuse Act[1] defines unauthorized access or tampering with federal or federal interest computers as a crime. The Electronic Communications Privacy Act[2] defines interfering with or disclosure of electronic mail or other kinds of electronic communication as against the law. Other statutes do not specifically mention computers, such as wire fraud,[3] various national security statutes, laws against theft and malicious mischief, and banking and securities laws. These statutes also can be applied in cases of computer crime where the individuals interfere with functioning of the systems, or use the computers to aid in the commission of some other crime.

Depending on which law is broken, the federal authorities who would investigate these offenses include the FBI, the Secret Service, and Department of Defense criminal investigation units. All would investigate the case for the U.S. Justice Department. If you suspect computer tampering that might fall under a federal law and are not sure who to contact, you should call the nearest U.S. Attorney's office. The staff there can recommend the appropriate law enforcement agency for you to notify.

2.1.2 State laws

Contacting state or local authorities is also important. If a federal statute has been violated, it is likely that a local statute is also involved. Your local law enforcement agencies can contact the appropriate federal agency for you. Almost all U.S. states currently have some form of computer crime law, although these laws are not uniform in their coverage, penalties, rules of evidence, or general composition. Many have not yet been tested in the courts, but were passed in reaction to perceived threats or recommendations.

Unfortunately, many state and municipal police agencies responsible for

[1] Section 1030 of Title 18 of the U.S. Code, usually abbreviated as 18 U.S.C. §1030.
[2] 18 U.S.C. §2701.
[3] 18 U.S.C. cd §1343.

investigating computer crimes often do not have officers with adequate technical training. The district or state's attorney who you hope will pursue criminal prosecution will need your assistance. One requirement common to almost every statute is that the intrusion or misuse of the computer be without authority. The evidence that there was no authorization, and that the defendant should have known better, can only come from you because it was your system and your responsibility. Your records and audit trail will be used to show exactly what happened. Computer crime cases are no different that other cases when it comes to the necessity of the the victim making a comprehensible complaint.

Although efforts towards computer literacy among law enforcement personnel are well underway, you must accept the fact that no outsider can be expected to understand your system as well as your own staff, nor can they explain it to a judge and jury without your help. Your active assistance can help ensure that the explanation is understood, and a conviction obtained.

2.1.3 Evidence

The collection of evidence is of critical importance in these crimes. Criminal charges cannot be filed and a trial cannot be won without conclusive evidence linking the perpetrator to the crime. According to law enforcement authorities who specialize in investigating and prosecuting these crimes, it is crucial that you contact authorities as soon as you suspect or discover any form of computer tampering. This is necessary to prevent any chance of the evidence disappearing, and to establish chains of custody. Do not assume it is minor—what you discover may be a small part of a widespread and on-going abuse of many different computer systems.

Although many law enforcement personnel may not have extensive computer experience, some of them may have considerably more expertise than your in-house computer operations personnel. In particular, they may have specialized knowledge about the collection and preservation of evidence that the average programmer probably lacks. After discovery of a computer break-in or a computer virus being unleashed on a system, there have been cases where the local staff attempted to recover or to investigate on their own. In the process, they had destroyed data, contaminating the potential evidence for the case to the point where it was unusable in a prosecution. If you discover a problem where you suspect criminal activity, it is important that you do not allow your own personnel to investigate beyond the point of ascertaining that there is a problem. Then contact appropriate law

enforcement agencies to obtain their advice and assistance.

Conclusive evidence is difficult to establish in criminal cases, since it must be proven to a jury beyond a reasonable doubt that the charged party is responsible for the crime. This may be especially difficult when prosecuting a computer virus author. Somehow you must link the coding and dissemination of the virus with a specific individual or set of individuals, and obtaining this evidence is not easy.

The fact that someone used an account and a password to access your system is not enough evidence to charge that individual with accessing your system illegally, introducing a virus, or performing some other malicious act. The fact that the account has been used does not necessarily identify the person who used it; depending on the integrity of your logging, you may not even be able to prove what account was used. Passwords can be cracked and accounts can be broken into, especially on systems where security is poor. At most, you may be able to use audit trails and other information to track down how the perpetrator entered your system. You may be able to identify who unleashed the code or performed certain actions, and if it was done in a malicious manner, you may be able to prosecute. Good auditing facilities and identification schemes are extremely important in this effort.

2.1.4 Impediments to prosecution

If investigation of a computer crime reveals that the perpetrator is a juvenile, it is unlikely that federal authorities will prosecute. Federal laws, courts, and prisons are not designed to handle juvenile offenders. It thus falls to state and local authorities to prosecute such crimes. This is another reason why it is important to include local authorities in investigations from the beginning.

Yet another problem with prosecution is that investigations for any kind of crime, and especially for computer-related crimes, may be personnel-intensive and expensive. They require specialized equipment, gathering considerable amounts of evidence, and a major expenditure of personnel time. Most law enforcement agencies (including federal) do not have budgets that are large enough to investigate all these crimes. Unless substantial damages can be shown, or unless the investigation is relatively straightforward, often local prosecutors will decide not to investigate or prosecute a case, especially if the evidence does not look conclusive. This leads to some problems, since without successful prosecutions as an deterrent, others may be encouraged to indulge in the same criminal behavior. Therefore, to prosecute an illegal

act successfully, you may need to invest a large amount of your own time and resources to aid in the investigation and the collection of evidence for the case. This should be done under the direction of, and with the cooperation of, your law enforcement personnel.

Even if enough evidence is collected, and your local or federal prosecutor files a case under one of these laws, there can be problems with proving a case in court. Cases of computer crime frequently require an explanation of considerable technological subtlety to a judge and jury, to enable them to understand the evidence and the damage involved. It may also be necessary to disclose confidential information that might have been stolen or damaged. When the theft of a trade secret is involved, it will require special handling to avoid exposing the secret in the course of the trial. This is especially critical when the defense involves the assertion that the material was not really a secret.

As a result of these considerations, computer crime cases can be difficult to conduct and to win. Furthermore, some of the laws that are applied in these cases result only in misdemeanor convictions that involve minor penalties.

One hope for successful criminal prosecution is the informed development of new laws at both the federal and state level. These laws should specify more clearly the kinds of prescribed behavior, the evidence required to bring charges and prosecute under the act, and how to deal with juveniles who are involved in these criminal activities. The new laws also should specify harsher penalties, depending on the severity of the crime involved. The case of someone writing a virus that infects hundreds of thousands of computers and erases the contents of their disks may cause only a few hundred dollars worth of damage on each system, but the total damage is ongoing and substantial. The statutory penalty should reflect the seriousness of such widespread damage. Appendix A contains a list of current state and federal statutes that may assist you in developing your security plans.

One trend that appears successful in some locales is to specify, as part of the damage recovery in lawsuits, that all the computer equipment belonging to the perpetrator be forfeited. This punishment is common in drug-related crimes, where paraphernalia and proceeds of drug-related activities are confiscated. These goods are either sold at auction or used by the police agencies. Similar tactics of confiscating all the computer-related equipment of the perpetrators of computer crimes on conviction may be appropriate to include in future laws.

2.2 Civil suits

Perhaps a more promising approach to dealing with computer criminals is filing civil suits (suing). Civil suits are brought by one entity against another, such as by a business against an individual, or by a business against another business, and seek redress for damages. These suits do not require violation of a specific law; instead, they seek to show that some form of common law (the law of torts) has been violated. A judge or jury may then award damages and penalties. Other relief, such as injunctions and forfeiture of property, may be instituted.[4]

If someone's computer has been broken into, data stolen or damaged, or a virus introduced, it is easy to show that the plaintiff has suffered a loss. If it can be proven that a specific individual was involved with such an incident, it may be possible to obtain some form of redress. The standard of proof in civil suits is not as stringent as in criminal cases, and thus may be easier to prepare and prove. Furthermore, your own personnel often can gather evidence for a case themselves, and they can serve as expert witnesses to document what occurred.

Civil cases can be expensive, and can take a long time to bring to trial. A civil suit coupled with preliminary injunctions may be the fastest relief available to you if you are the victim of someone who has caused substantial damage or is persistent in their activities. In particular, if you discover that someone is regularly hacking into your systems or writing viruses, and then find that other companies and individuals are affected as well, you might consider cosponsoring a lawsuit with them. If the costs of preparing such a lawsuit are shared by several companies, it may be easier to convince upper management to pursue a civil suit.

Furthermore, you may wish to combine a civil suit for damages with criminal prosecution. If a conviction is obtained in the criminal action first, that may be all that is needed for a successful civil prosecution, in addition to proof of damages.[5] Your attorney can advise you on the most appropriate course of action, including possible tradeoffs and consequences.

[4] Some state computer crime laws also provide for civil causes of action and relief.

[5] This depends on the venue and precedent. Some courts will not allow results of criminal actions admitted as evidence in civil suits.

3 Summary

This report has barely touched on the complexities involved with computer tampering and the law. This area is still evolving as new precedents are decided and new laws enacted. There is no substitute for the counsel of experienced attorneys, and it would be wise to seek out such advice as soon as it is needed. It may even be appropriate to obtain such counsel on a retainer basis, and regularly review both your legal options and vulnerabilities.

Key to any legal approach, however, is the decision to press ahead with prosecution. World-class attorneys and highly competent investigators can accomplish only a limited amount without the active cooperation of victims. Although it may be inconvenient and sometimes expensive, pursuing computer vandals can only help to establish further precedents and to discourage future attacks. If you fail to take appropriate measures it may leave you vulnerable to a civil suit should the perpetrators then use your system (or their experience with it) as a platform to launch further attacks. Avoiding prosecution may only encourage the perpetrators, and is a disservice to yourself and the profession.

A Further Information on Legal Aspects of Viruses

A.1 Federal Laws

There are many federal laws that can be used to prosecute criminal activity involving computers. As of 1 August 1989, there are at least two pieces of legislation before the U.S. House of Representatives to revise or augment existing laws, or to add new laws dealing with computer viruses and computer security. At least one more proposed law is known to be in preparation.

Currently, the primary law in effect is the Computer Fraud and Abuse Act, 18 U.S.C. §1030. Under this act, it is illegal to access a federal-interest computer knowingly and without authorization. There are six classifications of access described by the law, including access to financial information, data restricted under the Atomic Energy Act of 1954, and access with intent to defraud. Depending on the form of access, penalties may include prison terms ranging from one to 20 years. Fines up to $250,000 may also be levied in addition to jail terms. In addition to any other federal agency, the Secret Service is authorized to investigate offenses under this act.

The Electronic Communications Privacy Act of 1986, 18 U.S.C. §2701-2702 makes it illegal to access or interfere with electronic mail, storage, or transmission. This law might be used to prosecute individuals who obtain unauthorized access to a system with stored electronic communication, prevent others from accessing those systems, alter the electronic communication, or disclose it without permission. Penalties include fines of as much as $250,000 in addition to imprisonment.

18 U.S.C. §1029, the Credit Card Fraud Act of 1984, provides for prosecution of anyone who uses counterfeit or unauthorized access devices or codes (including account numbers and passwords) to gain access to a system in order to commit fraud. The definition of fraud could conceivably include the theft of computer services under someone else's login ID.

Other sections of Title 18 that could be used in the prosecution of computer criminals include:

§641 Theft of public money, property, or records

§646 Embezzlement by a bank employee

§659 Theft of goods or chattel in interstate commerce

§701 Unauthorized use of government identification

§793 Gathering, transmitting, or losing defense information

§794 Gathering or delivering defense information to aid foreign governments

§912 Impersonation of a government employee to obtain a thing of value

§1005 False entries in bank records

§1006 False entries in credit institution records

§1014 False statements in loan and credit applications

§1341 Mail fraud (use of U.S. mails to further a scheme to defraud)

§1343 Wire fraud (use of phone, wire, radio, or television transmissions to further a scheme to defraud)

§1344 Bank fraud

§1361 Malicious mischief to government property

§1905 Disclosure of confidential information (such as trade secrets)

§2071 Concealment, removal, or mutilation of public records

§2319 Criminal infringement of a copyright

§2510 et seq. Wiretapping (eavesdropping on computer communications)

Criminal prosecution may also occur under 15 U.S.C. §1693, the Electronic Funds Transfer Act.

Your U.S. Attorney will decide whether to prosecute under any of these (or other) statutes in the event of a criminal act. That decision will be based on available evidence, amount of loss, and probability of conviction. If evidence has been preserved (operations staff has not attempted to restore the system to an unaffected state), and an official investigation is begun soon after the crime is discovered, the likelihood of an indictment and conviction is enhanced.

A.2 State Laws

49 of the 50 states have laws against some form of computer abuse or unauthorized access; Vermont and the District of Columbia do not currently have laws specifically targeting computer crime. These statutes include a wide range of proscribed activities, including computer trespass, unauthorized alteration of data, denial of access, unauthorized use, theft of services, damage, theft, and attempts at any of the above. Not every state has implemented legislation against all of these activities. Penalties include fines ranging from a few hundred dollars up to $125,000, and prison terms from six months to 10 years. Many states, including California, Connecticut, Delaware, and Illinois provide for the forfeiture of computer equipment used in the commission of the crime.

The following is a list of statutes that might be used to prosecute someone who breaks into or damages your computer systems. Other state laws, including malicious mischief and trespass, may also be applied. In many states, the laws concerning computer crime are under review, and new or revised versions may soon be in force. You should consult your local authorities for the latest information on laws in your state.

Alabama Code §13A-8-100 et seq. (1988)

Alaska Statutes §11.46.200 (a), 11.46.740, 11.46.985, 11.46.990, 11.18.900 (1988)

Arizona Statutes §13-2301 and 13-2316 (1978 and 1988)

Arkansas Statutes §5-41-101 et seq.

California Penal Code §502 (1988)

Colorado Statutes §18-5.5-101 and 18-5.5-102 (1986)

Connecticut General Statutes §53a-250 et seq. (1985)

Delaware Code Title 11, §931 to 939 (1987)

District of Columbia, no provision

Florida Statutes §815.01 et seq. (1981)

Georgia Code §16-9-90 et seq. (1988)

Hawaii Statutes §708-890 et seq. (1985)

Idaho Code §18-2201, 18-2202, and 26-1220 (1987)

Illinois Criminal Code §15-1, 16D-1 et seq. (1988)

Indiana Code §35-43-1-4, 35-43-2-3 (1988)

Iowa Code §167, 716A.1 et seq. (1988)

Kansas Statutes §21-3704, 21-3745, 21-3755 (1988)

Kentucky Statutes §434.840 et seq. (1985)

Louisiana Statutes §14.73.1 et seq. (1986, 1989)

Maine Statutes Title 17-A, §357 (1983)

Maryland Code Article 27, §146, §45A

Massachusetts General Laws ch. 266, §30 (1988)

Michigan Statutes §28.529, 752.791 et seq.

Minnesota Statutes §609.87 et seq. (1989)

Mississippi Code §97-45-1 et seq. (1988)

Missouri Statutes §569.093 et seq. (1989)

Montana Code §45-2-101, 45-6-310 et seq. (1987)

Nebraska Statutes §28-1343 et seq. (1985)

Nevada Statutes §205.473 et seq. (1987)

New Hampshire Statutes §638.16 et seq. (1986)

New Jersey Statutes Chapter 20, Title 2C: §1. 20-34: Title 2A. §38A-1 et seq. (1987)

New Mexico Statutes §30-16A-1 et seq. (1984)

New York Penal Law §156.00 et seq.

North Carolina Genl. Statutes Art. 60 §14-453 et seq. (1986)

North Dakota Cent. Code §12.1-06.1-01 (3) et seq. (1987)

Ohio Code §2901.01, 2903, 2913.01 et seq., 2913.42, 2913.81 (1987)

Oklahoma Statutes Title 21 §1124, 1951 et seq. (1989)

Oregon Statutes §164.125 et seq. (1987)

Pennsylvania Statutes Title 18 §3933 (1988)

Rhode Island General Laws §11-52-1 et seq. (1981 and 1988)

South Carolina Code §16-16-10 et seq. (1985)

South Dakota Codified Laws §43-43B-1 et seq. (1984)

Tennessee Code §39-3-1401 et seq. (1988)

Texas Penal Code Title 7 §33.01 et seq. (1989)

Utah Code §76-6-701 et seq. (1988)

Vermont, currently no law

Virginia Code §18.2-152.1 et seq. (1988)

Washington Code §9A.48.100, 9A.52.100 et seq. (1989)

West Virginia §61-3C-1 (1989)

Wisconsin Statutes §943.70 (1988)

Wyoming Statutes §6-3-501 et seq. (1988)

A.3 Other Sources of Information

ADAPSO has compiled listings of all computer crime-related state laws as of September 1989. This document is entitled *Compendium of State and Federal Computer Crime Laws* and is available from ADAPSO offices:

ADAPSO
1300 North Seventeenth St.
Suite 300
Arlington, VA 22209-3899
(703) 522-5055

Commerce Clearing House publishes a two-volume set entitled *Guide to Computer Law*, containing summaries of federal laws, treaties, and regulations concerning computers. This includes issues of intellectual property, crime, licenses and leases, employee relations, and taxes. The books have removable pages, are updated on a periodic basis, and include recent court decisions—the material covered is comprehensive. Further information may be obtained from:

Commerce Clearing House, Inc.
4025 W. Peterson Avenue
Chicago, IL 60646

The National Institute of Justice has a number of publications, some free of charge, concerning computer crime investigation and prosecution. Three volumes of particular note are *Dedicated Computer Crime Units*, *Computer Crime: Criminal Justice Resource Manual*, and *Organizing for Computer Crime Investigation and Prosecution*. A list of available publications may be obtained by contacting the NIJ:

National Institute of Justice/NCJRS
Box 6000
Rockville, MD 20850
(800) 851-3420

A good survey of the problems associated with computer crime and the law is the report *Rogue Computer Programs—Viruses, Worms, Trojan Horses, and Time Bombs: Prank, Prowess, Protection or Prosecution?* by Anne W. Branscomb. The report contains citations to particular incidents of computer crime, and has a wealth of good references. The paper was issued by the Center for Information Policy Research, Harvard University.

The book, *Prevention and Prosecution of High Tech Crime,* by Stanley Arkin *et. al.* (Matthew Bender Press, Co., 1989) is another excellent reference to applicable law and legal strategy. This is a reference work well-suited for lawyers and law enforcement personnel as well as the interested computer professional.

Computer Law, by S. Lipner and S. Kalman (Merrill Publishing Co., 1989) is another good book on legal aspects, including material on intellectual property law.

Another helpful reference is the book *Computer Law* by Michael Scott (John Wiley & Sons, 1984). This is updated annually, and is useful in tracking new developments.

A publication for specialists in law enforcement and criminal justice entitled the *Police and Security Bulletin* is available from Lomond Publications. You may contact them at:

Lomond Publications
P.O. Box 88
Mt. Airy, MD 21771
(301) 829-1496

A few newsletters and journals are published that have major (or sole) emphasis on computers and crime/security. The *Computer Law Newsletter* can be ordered from:

28 State Street
Boston, MA 02109

The *Privacy Journal* may be ordered from:

P.O. Box 8844
Washington, DC 20003

The *Computer/Law Journal* may be ordered from:

Center for Computer Law
P.O. Box 3549
Manhattan Beach, CA 90266

A.4 Organizations

A.4.1 HTCIA

The High Technology Crime Investigators Association is a group of security professionals who meet to exchange information and conduct training

seminars for their members. The group is open only to individuals who are currently law enforcement personnel or corporate security officers. Prospective members may need references and must pass a background check. More information can be obtained from either of the two regional groups:

HTCIA Midwest
P.O. Box 243
Elmhurst, IL 60126

HTCIA
11515 South Colima Rd.
M-104
Whitier, CA 90604

A.4.2 NCCCD

The National Center for Computer Crime Data is devoted to the compilation and dissemination of data concerning computer crime and computer ethics. Its founder and director, J. J. BloomBecker, is a former assistant district attorney, and currently is the chair of the ACM Panel on Legal Issues. Unlike the other groups, the NCCCD cannot be "joined." However, their reports (which are highly recommended) may be ordered by contacting:

National Center for Computer Crime Data
2700 N. Cahuenga Blvd.
Suite 2113
Los Angeles, CA 90068
(213) 874-8233

A.4.3 NIST

The National Institute of Standards and Technology (formerly the National Bureau of Standards) has been charged with the development of computer security standards and evaluation methods for applications not involving the Department of Defense. Their efforts include research as well as developing standards. More information on their activities can be obtained by contacting:

NIST
Computer Security Division
A-216
Gaithersburg, MD 20899
(301) 975-3359

A.4.4 CERT

The Computer Emergency Response Team was established in late 1988 by DARPA to handle security problems in the Arpanet/Internet community. CERT has a 24-hour hotline for reports of security problems and break-ins. The CERT staff will follow up on these reports, and contact appropriate agencies and experts to investigate and respond to the difficulties reported. They will probably **not** respond to complaints of security problems involving personal computers of any kind, since the Internet does not involve PCs. However, CERT is very interested in reports of security problems with major machine operating systems and networking code (e.g., UNIX VMS, VM, NFS, TCP-IP, etc.). The Computer Emergency Response Team can be reached at:

cert@sei.cmu.edu (Internet e-mail)
(412) 268-7090 (24-hour hotline)
(412) 268-7080 (information)